THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

In re Progressive Leasing Breach Litigation	**MEMORANDUM DECISION AND ORDER GRANTING IN PART [56] DEFENDANT'S MOTION TO DISMISS** Case No. 2:23-cv-00783-DBB-CMR District Judge David Barlow Magistrate Judge Cecilia M. Romero

Defendant Progressive Leasing, LLC ("Defendant" or "Prog") moves to dismiss Plaintiffs'[1] consolidated class action complaint[2] under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).[3] For the following reasons, the court finds that the named Plaintiffs have standing to pursue their damages claims but not injunctive relief. Additionally, the court grants the motion in part and denies it in part for failure to state a claim.

BACKGROUND[4]

On or before September 18, 2023, Prog learned of a data breach on its network that occurred on or around September 11, 2023 (the "Data Breach").[5] Prog determined that, during the Data Breach, an unknown actor accessed files containing the personal identifiable information ("PII") of Plaintiffs.[6] On September 21, 2023, Prog's parent filed a Form 8-K with the Securities and Exchange Commission describing the Data Breach, including that "the

[1] The named Plaintiffs are Chad Boyd, Laura Robinson, Allison Ryan, Marty Alexander, Raymond Dreger, Ralph Maddox, Dawn Davis, Richard Guzman, Tyler Whitmore, Melanie Williams, and Stephen Hawes.
[2] Consolidated Class Action Compl. ("Compl."), ECF No. 39, filed April 19, 2024.
[3] Def.'s Mot. to Dismiss ("Mot."), ECF No. 56, filed June 24, 2024.
[4] At the motion to dismiss stage, the court accepts the complaint's factual allegations as true and views those facts in the light most favorable to the nonmoving party. *Moya v. Schollenbarger*, 465 F.3d 444, 455 (10th Cir. 2006).
[5] Compl. ¶ 7.
[6] *Id.* ¶ 8.

Company believes the involved data contained a substantial amount of personally identifiable information, including social security numbers, of Progressive Leasing's customers and other individuals."[7] The next day, reports began surfacing on the Internet that a ransomware group had acquired PII for 40 million individuals during the Data Breach, including Social Security numbers, bank routing numbers, and checking account numbers.[8] Within the next few days, another report emerged, stating that the ransomware group had obtained 18 terabytes of data, including "Full Company Data (Internal file shares, Software sources of Leasing Systems), 40 million customer records with full information, including their sensitive banking data," and that "Sample with proof of the exfiltrated data" had been leaked on the dark web.[9]

In late October, Prog began notifying Plaintiffs and Class Members of the Data Breach (the "Notice of Data Breach").[10] In the Notice of Data Breach, Prog informed Plaintiffs and Class Members that an unauthorized third party accessed sensitive information about Plaintiffs and Class Members, including name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email address.[11] The Notice of Data Breach further stated that "[a]s an added precaution, and to help protect your identity, we have secured the services of Experian to provide credit monitoring, identity restoration, and identity theft protection at no cost to you, as described in this letter."[12]

Within days after receipt of the Notices of Data Breach, Plaintiffs filed suit. On January 10, 2024 and March 29, 2024, the court granted two motions to consolidate eleven related

[7] *Id.* ¶ 9.
[8] *Id.* ¶ 10.
[9] *Id.* ¶ 11.
[10] *Id.* ¶¶ 12–13.
[11] *Id.* ¶¶ 42–44.
[12] *Id.* ¶ 42.

lawsuits into this action.[13] On April 19, 2024, Plaintiffs filed a consolidated class action complaint against Prog, alleging claims of negligence (Count I), breach of implied contract (Count II), declaratory judgment for injunctive relief (Count III), and violation of the California Consumer Privacy Act ("CCPA") (Count IV). As a result of the Data Breach, Plaintiffs allege that they suffered concrete harms stemming from the publishing of Plaintiffs' PII on the dark web, as well as attempted identity theft and fraud.[14] On June 24, 2024, Prog moved to dismiss Plaintiffs' consolidated complaint for a lack of subject matter jurisdiction and for failure to state a claim. The motion is now fully briefed.

LEGAL STANDARD

Dismissal is appropriate under Federal Rule of Civil Procedure 12(b)(1) when the court lacks subject matter jurisdiction over claims for relief asserted in the complaint. To avoid dismissal, plaintiffs must show that they suffered (1) an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that it is likely that the injury will be redressed by a favorable decision.[15] "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[16] "A 'concrete' injury must be 'de facto'; that is, it must actually exist."[17] A particularized interest "must affect the plaintiff in a personal and individual way."[18] Generally, "threatened injury must be certainly impending to constitute

[13] Mem. Decision and Order Granting Mot. to Consolidate Cases, ECF No. 22, dated January 10, 2024; Mem. Decision and Order Granting Mot. to Consolidate Cases, ECF No. 34, dated March 29, 2024.
[14] *E.g.*, Compl. ¶¶ 10–11, 96–97, 111, 152, 178, 193–98, 205.
[15] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-61 (1992).
[16] *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016), *as revised* (May 24, 2016) (quoting *Lujan*, 504 U.S. at 560).
[17] *Id.* at 340.
[18] *Id.* at 339.

injury in fact," although the Supreme Court has noted that in some cases it has "found standing based on a 'substantial risk' that the harm will occur."[19]

The traceability element of standing "requires a plaintiff to 'allege a substantial likelihood that the defendant's conduct caused [the] plaintiff's injury in fact.'"[20] "The injury must not be 'the result of the independent action of some third party not before the court'" nor can a plaintiff rely on a "speculative chain of possibilities."[21] "The burden of establishing subject matter jurisdiction is on the party asserting jurisdiction."[22] Notwithstanding, a court must accept as true all well-pleaded facts and construe all reasonable allegations in the light most favorable to the plaintiff.[23]

Dismissal is appropriate under Federal Rule of Civil Procedure 12(b)(6) when the complaint, standing alone, is legally insufficient to state a claim on which relief may be granted. Each cause of action must be supported by sufficient, well-pled facts to be plausible on its face.[24] In reviewing a complaint on a Rule 12(b)(6) motion to dismiss, factual allegations are accepted as true and reasonable inferences are drawn in a light most favorable to the plaintiff.[25] But the court disregards "assertions devoid of factual allegations" that are nothing more than "conclusory" or "formulaic recitation[s]" of the law.[26]

---

[19] *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 410, 414 n.5 (2013).
[20] *Masterson v. IMA Fin. Grp., Inc.*, No. 2:23-cv-02223-HLT-ADM, 2023 WL 8647157, at *3 (D. Kan. Dec. 14, 2023) (quoting *Santa Fe All. for Pub. Health & Safety v. City of Santa Fe, N.M.*, 993 F.3d 802, 814 (10th Cir. 2021)).
[21] *Blood v. Labette Cnty. Med. Ctr.*, No. 5:22-cv-04036-HLT-KGG, 2022 WL 11745549, at *4 (D. Kan. Oct. 20, 2022) (quoting *Clapper*, 568 U.S. at 414)).
[22] *Port City Props. v. Union Pac. R.R. Co.*, 518 F.3d 1186, 1189 (10th Cir. 2008).
[23] *United States v. Colorado Supreme Court*, 87 F.3d 1161, 1164 (10th Cir. 1996) (citations omitted).
[24] *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).
[25] *GFF Corp. v. Associated Wholesale Grocers, Inc.*, 130 F.3d 1381, 1384 (10th Cir. 1997).
[26] *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 681 (2009).

DISCUSSION

I. ARTICLE III STANDING

Data breach cases involve unique issues of Article III standing, particularly regarding what constitutes injury in fact. Questions arise as to whether the fact that a cybercriminal has obtained an individual's sensitive PII alone is sufficient, or whether the individual needs to allege misuse of the data, such as through identity theft, fraud, or posting the information on the dark web. Similarly, courts grapple with whether the misuse of some subset of the stolen data affords other plaintiffs an injury in fact based on the increased likelihood that the plaintiffs' data will be misused in the near future.

As another district court in the Tenth Circuit recently observed, "[i]t appears the Tenth Circuit has not yet addressed Article III standing in a data breach case, but almost all other circuits have done so."[27] The court will first discuss some of the earlier decisions from other circuits grappling with standing following a data breach. Next, the court will summarize two relevant Supreme Court opinions—*Clapper v. Amnesty Intern. USA*[28] and *TransUnion LLC v. Ramirez*.[29] Then the court will review some of the more recent opinions analyzing data breach standing in light of *TransUnion*. Finally, the court will analyze the allegations in this case.

A. Relevant Circuit Court Decisions Pre-*TransUnion*

A few months prior to *TransUnion*, the Eleventh Circuit analyzed cases conferring standing after a data breach based on an increased risk of theft or misuse and noted that they "included at least some allegations of actual misuse or actual access to personal data."[30] For

---

[27] *Maser v. Commonspirit Health*, No. 1:23-cv-01073-RM-SBP, 2024 WL 2863579, at *4 (D. Colo. Apr. 16, 2024).
[28] 568 U.S. 398, 410 (2013).
[29] 594 U.S. 413, 436 (2021).
[30] *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340 (11th Cir. 2021); *see also McCombs*, 676 F.Supp.3d at 1070 (stating that nearly all cases where plaintiffs had standing in data breach cases involved allegations that they suffered actual misuse of the data accessed). The Eleventh Circuit noted one exception in *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629 (7th Cir. 2007) but deemed the case an outlier because (i) it was pre-

example, in *Remijas v. Neiman Marcus, LLC*,[31] plaintiffs brought a class action involving the unauthorized exposure of 350,000 credit card numbers from defendant's database and fraudulent charges on 9,200 of the cards.[32] The Seventh Circuit held that even those plaintiffs who had not experienced fraudulent charges had standing because their risk of future injury was substantial.[33] The court reasoned that "customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur."[34]

Similarly, in *Galaria v. Nationwide Mut. Ins. Co.*,[35] one plaintiff discovered three unauthorized attempts to open credit cards in his name using PII obtained from a data breach.[36] The Sixth Circuit held that all plaintiffs had standing because the "theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of 'possible future injury' or 'objectively reasonable likelihood' of injury that the Supreme Court has explained are insufficient."[37] It explained that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."[38]

Next, in *Attias v. Carefirst, Inc.*,[39] the D.C. Circuit found standing in a data breach case because "a substantial risk of harm exists already, simply by virtue of the hack and the nature of

---

Clapper; and (ii) none of the Seventh Circuit's data breach cases following *Clapper* even cite *Pisciotta*. *Tsao*, 986 F.3d at 1341.

[31] 794 F.3d 688 (7th Cir. 2015).

[32] *Id.* at 690.

[33] *Id.* at 693.

[34] *Id.*

[35] 663 F. App'x 384 (6th Cir. 2016).

[36] *Id.* at 387.

[37] *Id.* at 388.

[38] *Id.*

[39] 865 F.3d 620 (D.C. Cir. 2017).

the data that the plaintiffs allege was taken."[40] The complaint also included an allegation that two of the named plaintiffs had suffered identity theft as a result of the breach.[41]

Likewise, in *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*,[42] cybercriminals applied for credit cards using Plaintiffs' stolen PII.[43] As a result, Plaintiffs alleged they faced an imminent threat of future harm from identity theft and fraud.[44] The Fourth Circuit held that "[b]ecause the injuries alleged by the Plaintiffs are not speculative, the costs of mitigating measures to safeguard against future identity theft" are sufficient to constitute an injury in fact.[45] The court maintained that "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft."[46]

Continuing this trend, the Ninth Circuit in *In re Zappos.com, Inc.*,[47] held that plaintiffs sufficiently alleged standing based on the risk of identity theft even though they, unlike other plaintiffs in the case, did not allege that the hackers used their PII to conduct subsequent financial transactions.[48] The court explained that the alleged harms of those whose PII was misused "undermines [defendant's] assertion that the data stolen in the breach cannot be used for fraud or identity theft."[49]

And finally, another Eleventh Circuit decision, *In re Equifax Inc. Customer Data Security Breach Litigation*[50] recognized that some Plaintiffs alleged that they already had their identities

[40] *Id.* at 629.
[41] *Id.* at 626 n.2.
[42] 892 F.3d 613 (4th Cir. 2018).
[43] *Id.* at 618.
[44] *Id.*
[45] *Id.* at 622.
[46] *Id.* at 621.
[47] 888 F.3d 1020 (9th Cir. 2018).
[48] *Id.* at 1023.
[49] *Id.* at 1027.
[50] 999 F.3d 1247 (11th Cir. 2021).

stolen and concluded that these allegations of "actual identity theft support the sufficiency of all Plaintiffs' allegations that they face a *risk* of identity theft."[51]

In at least slight contrast to these sentiments, the Eighth Circuit declined to find that the fraud one plaintiff experienced sufficed to show a substantial risk of future misuse of other plaintiffs' stolen credit card data. In *In re SuperValu, Inc.*,[52] the Eighth Circuit addressed a data breach case where cybercriminals accessed the plaintiffs' credit card information.[53] One plaintiff alleged that he noticed a fraudulent charge on his credit card as a result of the data breach and thus had standing.[54] The remaining plaintiffs, however, argued that the theft of their credit card information created a substantial risk that they will suffer identity theft in the future.[55] In rejecting this argument, the court noted that the stolen credit card information did not include Social Security numbers, birth dates, or driver's license numbers and thus, "generally cannot be used alone to open unauthorized new accounts."[56] The court also found that there was no substantial risk of account fraud based on a GAO report that found that, of the 24 largest data breaches reported between January 2000 and June 2005, only four resulted in some form of identity theft and only three of those were believed to be incidents of account fraud.[57]

On the other hand, circuit courts generally have not found standing where no plaintiff alleged misuse. For example, in *Reilly v. Ceridian Corp.*,[58] the Third Circuit held that plaintiffs had no injury because they did not allege misuse of the compromised data.[59] The court explained that plaintiffs' allegations of a "hypothetical, future injury" were insufficient because they "rely

[51] *Id.* at 1263.
[52] 870 F.3d 763 (8th Cir. 2017).
[53] *Id.* at 766.
[54] *Id.* at 767.
[55] *Id.* at 770.
[56] *Id.*
[57] *Id.* at 771.
[58] 664 F.3d 38 (3d Cir. 2011).
[59] *Id.* at 45 ("In data breach cases where no misuse is alleged . . . there has been no injury.").

on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [plaintiffs] by making unauthorized transactions in [plaintiffs'] names."[60]

Similarly, in *Tsao v. Captiva MVP Rest. Partners*, LLC,[61] the Eleventh Circuit found that the plaintiff did not allege an injury in fact because he "did not point to any specific instances in which his—*or any other class member's*—identity was stolen, cards were fraudulently charged, or data was misused."[62] The court stated that "without specific evidence of *some* misuse of class members' data," plaintiff's burden "will be difficult to meet."[63]

Finally, in *McMorris v. Carlos Lopez & Assocs., LLC*,[64] an employee accidently sent all employees of a company an email containing current and former employees' PII.[65] The Second Circuit held that mere increased risk of identity theft can be a concrete injury, although courts are more likely to so conclude when plaintiffs can show that "at least some part of the compromised dataset has been misused – even if plaintiffs' *particular* data subject to the same disclosure incident has not yet been affected."[66] Nonetheless, the court found that plaintiffs' allegations were insufficient because the data was not intentionally targeted or misused in any way.[67]

In sum, the pre-*TransUnion* case law overwhelmingly concludes that where there is no misuse of any plaintiff's PII, injury will be particularly difficult to establish.[68] And, with the

---

[60] *Id.* at 42.
[61] 986 F.3d 1332 (11th Cir. 2021).
[62] *Id.* at 1336 (emphasis added).
[63] *Id.* at 1344.
[64] 995 F.3d 295 (2d Cir. 2021).
[65] *Id.* at 298.
[66] *Id.* at 301.
[67] *Id.* at 303–304.
[68] *E.g.*, *Tsao*, 986 F.3d at 1343 ("Of course, as our sister Circuits have recognized, evidence of actual misuse is not necessary for a plaintiff to establish standing following a data breach.").

exception of the Eighth Circuit's opinion in *In re SuperValu, Inc.*,[69] courts generally consider allegations of actual misuse by some plaintiffs to support a substantial risk of future misuse of other plaintiffs' PII from the same compromised data set.

B. Relevant Supreme Court Decisions

Prior to *TransUnion*, most courts discussing future injury in the data breach context relied on *Clapper v. Amnesty Int'l USA*.[70] *Clapper* involved a group of plaintiffs whose work requires them to engage in sensitive international communications with individuals who they believe are likely targets of government surveillance.[71] The Supreme Court found that they did not have standing based on a future injury that their communications might be surveilled because a "'threatened injury must be *certainly impending* to constitute injury in fact,'" and "'[a]llegations of possible future injury' are not sufficient."[72] In doing so, the court found that an "objectively reasonable likelihood" is insufficient,[73] although the court maintained that "[i]n some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[74] Further, a plaintiff cannot establish an imminent future injury when they "rel[y] on a highly attenuated chain of possibilities" or "speculation about the decisions of independent actors."[75]

The Supreme Court shed more light on proving a concrete injury based on future harm in *TransUnion LLC v. Ramirez*.[76] In *TransUnion*, a class of plaintiffs sued TransUnion under the Fair Credit Report Act for maintaining inaccurate credit reports.[77] TransUnion provided certain

[69] 870 F.3d 763 (8th Cir. 2017).
[70] 568 U.S. 398 (2013).
[71] *Id.* at 401.
[72] *Id.* at 409.
[73] *Id.* at 410.
[74] *Id.* at 414 n.5.
[75] *Id.* at 410–414.
[76] 594 U.S. 413 (2021).
[77] *TransUnion*, 594 U.S. 417.

of these plaintiffs' inaccurate credit reports to third parties.[78] For the remaining plaintiffs, TransUnion only maintained the inaccurate credit reports in its internal system and never provided the information to third parties.[79]

The Court had "no trouble" holding that the first group of plaintiffs alleged a concrete injury, reasoning that the disclosure "bears a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—namely, the reputational harm associated with the tort of defamation."[80] In contrast, the remaining plaintiffs did not have standing because "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm."[81]

In so finding, the Court rejected plaintiffs' argument that they had standing because there was a "material risk that [inaccurate credit report] information would be disseminated in the future to third parties and thereby cause them harm."[82] Further, the court specified that *Clapper* involved a suit for injunctive relief (where future harm can constitute an injury), and plaintiffs "must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)."[83] The Court found that the plaintiffs "did not demonstrate that the risk of future harm materialized," nor did they "present evidence that the class members were independently harmed by their exposure to the risk itself[.]"[84] That TransUnion had already provided inaccurate credit reports to third parties of 1,853 plaintiffs who did have standing was insufficient to provide standing to the remaining plaintiffs. Accordingly,

---

[78] *Id.* at 432.
[79] *Id.* at 437.
[80] *Id.* at 432.
[81] *Id.* at 436.
[82] *Id.* at 435.
[83] *Id.* at 431, 435.
[84] *Id.* at 437.

the court concluded that plaintiffs "did not factually establish a sufficient risk" that TransUnion would release their information to third parties in the future and their claims were too speculative to support Article III standing.[85]

C. Post-*TransUnion* Decisions

The Tenth Circuit has not addressed whether "the mere fact that a data breach occurred necessarily mean[s] that a customer has suffered a concrete injury, or [whether] something more [is] required[.]"[86] In light of *TransUnion*, the U.S. District Court for the Western District of Oklahoma in *Legg v. Leaders Life Insurance Company* opined that "it is far from clear that any case finding a concrete injury based merely on an abstract risk of future identity theft is still good law, at least with respect to a claim for damages."[87] Following *TransUnion*, courts in this district have consistently declined to find standing absent any allegations of actual misuse.[88]

The court in *Legg* held that "[g]iven the holding in *TransUnion*," the plaintiff did not have standing for damages where his claim was not premised on "any actual fraud or identity theft that occurred as a result of the data breach, but on the risk that fraud or identity theft may occur in the future."[89] "Crucially, Plaintiff does not allege that he or any other class member has been the victim of identity theft or fraud."[90] The court stated that "[e]ven accepting as true Plaintiff's allegations about the nature of the breach – that it was an intentional attack by

[85] *Id.* at 437–38.
[86] *Legg v. Leaders Life Ins. Co.*, 574 F.Supp.3d 985, 989 (W.D. Okla. 2021).
[87] *Id.* at 993.
[88] *See Deevers Stoichev v. Wing Fin. Servs., LLC*, No. 22-cv-0550-CVE-JFJ, 2023 WL 6133181, at *6 (N.D. Okla. Sept. 19, 2023) ("While some circuits have found that misuse by a third-party, while sufficient, is not necessary on its own to establish imminence, the majority of courts, including district courts in this circuit, have concluded that plaintiffs must allege actual misuse of to demonstrate they face an imminent risk of fraud.").
[89] *Legg*, 574 F.Supp.3d at 993.
[90] *Id.* at 988.

cybercriminals – Plaintiff only pleads facts showing that there is a non-imminent risk of possible future injury following the data breach. This is not sufficient to confer standing."[91]

Similarly, in *C.C. v. Med-Data, Inc.*,[92] plaintiff's PII, including Social Security number, was "uploaded to a public facing website" following a data breach.[93] Notably, the plaintiff did not allege any misuse of the data or that it was uploaded to the dark web.[94] As a result, the court held that the plaintiff did not have standing because a "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft."[95] The court also predicted that the Tenth Circuit "would follow the line of cases where outcome depends on whether plaintiffs have alleged misuse of their data."[96]

Likewise, in *McCombs v. Delta Group Electronics, Inc.*,[97] a plaintiff brought a class action after a cybercriminal hacked Delta's security systems and accessed data that included plaintiff's first and last name, Social Security number, driver's license number, and financial account number.[98] The plaintiff alleged, among other things, general future risks of harm associated with identity theft that had yet to materialize based on her belief that her PII "may end up for sale on the dark web" or may lead to "targeted marketing."[99] In determining that the plaintiff lacked standing, the court "followed the majority view concluding that a plaintiff does not suffer an injury in fact where their PII is accessed through a data breach but no direct harm results."[100] It explained that following *TransUnion*, "the mere possibility of a potential

---

[91] *Id.* at 994.
[92] No. 21-cv-2301-DDC-GEB, 2022 WL 970862 (D. Kan. Mar. 31, 2022).
[93] *Id.* at *1.
[94] *See id.* at *7.
[95] *Id.*
[96] *Id.* at *4.
[97] 676 F.Supp.3d 1064 (D.N.M. 2023).
[98] *Id.* at 1067.
[99] *Id.* at 1068.
[100] *Id.* at 1071 (citing cases).

unrealized injury, without more, does not confer standing."[101] As such, the court refused "to credit the possibility that McCombs' PII will be used by an unknown cybercriminal to potentially commit fraud or identity theft."[102]

The court in *F.S. v. Captify Health, Inc.*[103] recently came to the same conclusion because the plaintiff "failed to allege any facts about data misuse—of his data or anyone else's—that could nudge plaintiff's chances of future injury into an imminent one."[104] Each of these cases involved a single named plaintiff without any co-plaintiffs alleging misuse of their PII.[105]

Consistent with this, multiple circuits have found that actual misuse of PII is not required for every plaintiff individually and that plaintiffs can obtain standing based on actual misuse of other plaintiffs' PII. In *Webb v. Injured Workers Pharmacy, LLC*,[106] the First Circuit grappled with whether two plaintiffs had standing following a data breach where only one of them alleged actual misuse. The court found that one plaintiff suffered an injury in fact based on allegations that her PII was used to file a fraudulent tax return.[107]

As the First Circuit acknowledged, the standing inquiry regarding the other plaintiff (who did not allege misuse) was "more difficult."[108] Nonetheless, the court concluded that, "in light of the plausible allegations of some actual misuse, the complaint plausibly alleges a concrete injury in fact based on the material risk of future misuse of [her] PII and a concrete harm caused by

[101] *Id.* at 1072.
[102] *Id.*
[103] No. 23-1142-DDC-BGS, 2024 WL 1282437 (D. Kan. Mar. 26, 2024).
[104] *Id.* at *5.
[105] *See, e.g.*, *id.* (plaintiff did not allege misuse of his data "or anyone else's"); *Legg*, 574 F.Supp.3d at 998 ("Crucially, Plaintiff does not allege that he *or any other class member* has been the victim of identity theft or fraud.") (emphasis added).
[106] 72 F.4th 365 (1st Cir. 2023).
[107] *Id.* at 373.
[108] *Id.* at 374.

exposure to this risk."[109] The court explained that plaintiffs whose information is compromised in a targeted data breach "face a real risk of misuse of their information . . . by thieves intending to use the information to their financial advantage."[110] "[T]he actual misuse of a portion of the stolen information increases the risk that other information will be misused in the future."[111] A few district courts in this circuit have come to the same conclusion.[112]

After finding that plaintiffs faced an imminent and substantial future risk of misuse of their PII, the First Circuit "join[ed] other circuits in concluding that time spent responding to a data breach can constitute a concrete injury sufficient to confer standing, at least when that time would otherwise have been put to profitable use."[113] The court distinguished *Clapper* because "this is not a case where the plaintiffs seek to 'manufacture standing by incurring costs in anticipation of non-imminent harm.'"[114]

The Second Circuit in *Bohnak v. Marsh & McLennan Companies, Inc.*[115] repeated its past observation that courts are more likely to conclude that a plaintiff has established a "substantial risk of future injury" where some part of the compromised dataset has been misused—even if a plaintiff's own data has not[116]—but then seemingly went a step further. In *Bohnak*, the Second Circuit concluded that the plaintiff had standing solely based on her allegation that an unauthorized third party accessed her name and Social Security number through a targeted data

---

[109] *Id.* The Supreme Court in *TransUnion* stated, "a material risk of future harm can satisfy the concrete-harm requirement," at least as to injunctive relief, when "the risk of harm is sufficiently imminent and substantial." *TransUnion*, 594 U.S. at 435.
[110] *Webb*, 72 F.4th at 375.
[111] *Id.*
[112] *See Krant v. UnitedLex Corp.*, No. 23-2443-DDC-TJJ, 2024 WL 3511300, at *2 n.2 (D. Kan. July 23, 2024) (concluding that the named plaintiffs' allegations of harm create an imminent risk of harm and support standing for other plaintiffs); *Maser*, 2024 WL 2863579, at *6 ("Thus, cases that involve targeted breaches, fraud-sensitive data, and actual misuse (as to at least one named plaintiff) easily meet the Article III standing requirement at the pleading phase.").
[113] *Id.* at 377.
[114] *Id.*
[115] 79 F.4th 276 (2d Cir. 2023).
[116] *Id.* at 288.

breach, even though she did not allege misuse.[117] Relying on *TransUnion* for the view that intangible harms, including disclosure of private information, can be concrete, the Second Circuit likened exposure of the plaintiff's PII to hackers with public disclosure of private facts.[118] The Second Circuit explained that the disclosure of one's PII bears a relationship to an injury with a "close historical or common-law analogue" and that analogue need not be "an exact duplicate."[119]

In addition, the court opined that the plaintiff also suffered a concrete harm based on the risk of future harm because the plaintiff alleged that she incurred out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, lost time, and other opportunity costs associated with attempting to mitigate the consequences of the data breach.[120] As in *Webb*, the court concluded that because there was a substantial and imminent risk of harm, *Clapper's* prohibition on manufacturing standing did not apply.[121] In finding a substantial and imminent risk of harm, the Second Circuit applied *McMorris*,[122] which established three non-exhaustive factors to consider, including (1) whether plaintiffs' data exposure was as a result of a targeted or accidental breach; (2) whether any portion of the dataset has already been misused; and (3) whether the type of data exposed is sensitive, such that there is a high risk of identity theft or fraud.[123] In analyzing these factors, the Second Circuit in *Bohnak* concluded that the plaintiff faced an imminent risk of injury because her PII was exposed as a result of a targeted breach and the compromised PII includes her name and Social Security number, which is

[117] *Id.* at 280.
[118] *Id.* at 285.
[119] *Id.* at 286.
[120] *Id.*
[121] *Id.* at 287.
[122] 995 F.3d 295 (2d Cir. 2021).
[123] *Id.* at 303. *Bohnak* clarified that *TransUnion* is the touchstone for determining concrete injury, while *McMorris* is the touchstone for determining an "actual or imminent" injury. *Bohnak*, 79 F.4th at 283.

"exactly the kind of information that gives rise to a high risk of identity theft."[124] The court recognized that the plaintiff did not allege any known misuse of information in the dataset, but "such an allegation is not necessary to establish that an injury is sufficiently imminent to constitute an injury in fact."[125]

The Third and Eleventh Circuits also grappled with data breach cases post-*TransUnion*. In *Clemens v. ExecuPharm Inc.*,[126] 48 F.4th 146, 155–56 (3d Cir. 2022), hackers posted the plaintiff's PII on the dark web.[127] The Third Circuit concluded that because it "can reasonably assume that many of those who visit the Dark Web . . . do so with nefarious intent, it follows that Clemens faces a substantial risk of identity theft or fraud by virtue of her personal information being made available on underground websites."[128] As in *Bohnak*, the Third Circuit analogized the harm to disclosure of private information and further stated that because the risk of identity theft or fraud was imminent, emotional distress or money spent on mitigation measures constitute a concrete injury.[129] Similarly, in *Green-Cooper v. Brinker Int'l, Inc.*,[130] hackers took plaintiffs' credit card data and posted it on the dark web.[131] Deeming this allegation "critical" and the kind of misuse that was missing in *Tsao*, the Eleventh Circuit held that plaintiffs established a concrete injury and a substantial risk of future injury.[132]

In summary, although the pre- and post-*TransUnion* district and circuit court cases are not entirely uniform, common trends appear. The majority of courts both pre- and post-

[124] *Bohnak*, 79 F.4th at 289.
[125] *Id.*
[126] 48 F.4th 146 (3d Cir. 2022).
[127] *Id.* at 150.
[128] *Id.* at 157.
[129] *Id.* at 155–56.
[130] 73 F.4th 883 (11th Cir. 2023).
[131] *Id.* at 889. Specifically, the data was posted on Joker Stash, an online marketplace for stolen payment data. *Id.* at 886.
[132] *Id.* at 889–90.

TransUnion require some evidence of misuse of PII, such as posting PII on the dark web, identity theft, or fraud, to find an imminent injury—the Second Circuit in *Bohnak* being a notable exception.[133] Further, many courts have generally allowed all plaintiffs to demonstrate standing at the motion to dismiss stage following an allegation that other plaintiffs' data has been misused, based on the premise that actual misuse of a portion of the stolen dataset increases the risk that other information in the same dataset will be misused in the future.[134] Of course, the Eighth Circuit's pre-*TransUnion* holding in *In re SuperValu, Inc.*[135] is notably an exception, although it relied on data from a GAO study that is now approximately 20 years old.

After review of the underlying case law and reasoning, the court adopts what appears to be the two majority rules—first, misuse is generally necessary to obtain standing; second, at the pleadings stage, allegations of misuse by some plaintiffs often can suffice to plausibly show that other plaintiffs' injury is imminent. Once the injury is deemed imminent, plaintiffs can potentially allege a concrete injury based on lost money and time spent on mitigating the imminent harm, and perhaps the emotional distress occasioned by the imminent misuse. With these conclusions in mind, the court turns to Plaintiffs' allegations.

D. Analysis of Plaintiffs' Allegations

In their consolidated complaint, Plaintiffs allege the following injuries as a result of the Data Breach: (i) that their PII was or might be placed or sold on the dark web which creates heightened risk of identity theft or fraud; (ii) lost or diminished value of PII; (iii) lost time and out-of-pocket expenses associated with attempting to mitigate potential future harms associated

[133] In potential contrast to *Bohnak*, the First Circuit in *Webb* stated, "[w]e do not hold that individuals face an imminent and substantial future risk in every case in which their information is compromised in a data breach. But on the facts alleged here, the complaint has plausibly demonstrated such a risk." *Webb*, 72 F.4th at 376.
[134] *See, e.g.*, *Webb*, 72 F.4th at 375; *Bohnak*, 79 F.4th at 288; *Krant v. UnitedLex Corp.*, No. 23-2443-DDC-TJJ, 2024 WL 3511300, at *2 n.2 (D. Kan. July 23, 2024); *Maser*, 2024 WL 2863579, at *6.
[135] 870 F.3d 763 (8th Cir. 2017).

with the Data Breach; (iv) lost benefit of the bargain with Prog; (v) inconvenience via spam calls, texts, and emails; (vi) emotional distress such as anxiety and stress; and (vii) their PII was compromised or taken during the Incident.[136]

Prog argues that Plaintiffs' consolidated complaint must be dismissed because Plaintiffs have not plead facts demonstrating they have Article III standing. In doing so, Prog splits the Plaintiffs into two groups based on whether a Plaintiff alleges misuse of their information. Four of the eleven named Plaintiffs—Chad Boyd, Laura Robinson, Allison Ryan, and Marty Alexander—allege misuse of their PII (the "Alleged-Misuse" Plaintiffs), but according to Prog, lack concrete injuries and fail to allege the injuries are traceable to the Data Breach. The remaining seven named Plaintiffs—Raymond Dreger, Ralph Maddox, Dawn Davis, Richard Guzman, Tyler Whitmore, Melanie Williams, and Stephen Hawes—do not allege any instances of unauthorized use, or misuse, of the PII that was involved in the Data Breach (the "Non-Misuse" Plaintiffs).

In their Opposition, Plaintiffs argue that they have standing based on (i) the placement of Plaintiffs' PII on the dark web; (ii) the identity theft or fraud experienced by the Alleged-Misuse Plaintiffs; and (iii) the increased risk of identity theft based on the actual fraud or identity theft experienced by some Plaintiffs.

1. Standing Based on Publication on the Dark Web

"[A] mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft,"[137] and Plaintiffs do not argue otherwise. Plaintiffs contend that they "were all injured by the posting of their PII, including their Social

[136] Compl. ¶¶ 11, 15, 17, 19, 47, 79, 88–92, 109–14, 121–25, 131–36, 143–46, 152–58, 205–09, 253–55.
[137] *C.C. v. Med-Data Inc.*, No. 21-cv-2301-DDC-GEB, 2022 WL 970862, at *7 (D. Kan. Mar. 31, 2022) (quoting *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018)).

Security numbers and bank account numbers, on the dark web."[138] In support, they point to paragraphs 10 and 11 of the consolidated complaint:

> 10. On or around September 22, 2023, reports began surfacing on the Internet that the BlackCat/ALPHV ransomware group had acquired PII for 40 million individuals during the Data Breach, including Social Security numbers, bank routing numbers, and checking account numbers.[139]
>
> 11. On or around September 23-25, 2023, another report surfaced on the Internet stating that 18 terabytes of data had been exfiltrated during the Data Breach, including "Full Company Data (Internal file shares, Software sources of Leasing Systems), 40 million customer records with full information, including their sensitive banking data," and that "Sample with proof of the exfiltrated data" had been leaked on the dark web.[140]

Plaintiffs overstate these allegations. These paragraphs only state that a *sample* of Prog's data was posted to the dark web. They do not state that any of the named Plaintiffs' own personal information was contained within that sample. This is further supported by Plaintiffs' allegation that their unencrypted PII "may end up for sale on the dark web."[141] Notwithstanding, three of the seven Non-Misuse Plaintiffs do in fact allege that their information was posted on the dark web following the Data Breach, including Mr. Maddox,[142] Ms. Williams,[143] and Mr. Hawes.[144]

Mr. Maddox alleges that he "suffered actual injury in the form of his PII being disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach";[145] Ms. Williams alleges that her "PII [was] compromised and/or stolen as a result of the Data Breach," and she "was recently alerted to her information, including the PII compromised in the Data Breach, being found on the dark web";[146] and Mr. Hawes

[138] Pls.' Opp'n to Def.'s Mot. to Dismiss ("Opp'n"), ECF No. 64, filed on August 9, 2024.
[139] Compl. ¶ 10.
[140] *Id.* ¶ 11.
[141] *Id.* ¶ 47.
[142] *Id.* ¶ 111.
[143] *Id.* ¶ 152.
[144] *Id.* ¶ 205.
[145] *Id.* ¶ 111.
[146] *Id.* ¶ 152.

alleges that he "was deprived of [the value of his PII] when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web."[147] Mr. Maddox and Mr. Hawes further allege that they are "very careful about sharing [their] PII."[148]

Prog does not appear to argue that the posting of Plaintiffs' stolen PII on the dark web *as a result of* the Data Breach would not constitute an injury in fact.[149] Indeed, "allegations that the plaintiffs' PII was available for sale on the Dark Web following a data breach—and could therefore be purchased by cybercriminals at any moment to commit identity theft or fraud—provide[s] strong support for the conclusion that those plaintiffs had established an Article III injury in fact."[150] Moreover, the publication of Plaintiffs' PII on the dark web is akin to disclosure of private information, which the Supreme Court specifically recognized as a concrete intangible harm.[151]

Instead, Prog challenges traceability, arguing that Plaintiffs' allegations are insufficient because they "are non-specific and carefully crafted to acknowledge the possibility that their

---

[147] *Id.* ¶ 205.
[148] *Id.* ¶¶ 107, 202.
[149] *See* Reply 2–4.
[150] *McMorris*, 995 F.3d at 302; *see also Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889–90 (11th Cir. 2023) ("The fact that hackers took credit card data and corresponding personal information . . . and affirmatively posted that information for sale on [the dark web] is the misuse for standing purposes that we said was missing in *Tsao*."); *Clemens*, 48 F.4th at 157 (3d Cir. 2022) ("Because we can reasonably assume that many of those who visit the Dark Web, and especially those who seek out and access [the hacking group's] posts, do so with nefarious intent, it follows that Clemens faces a substantial risk of identity theft or fraud by virtue of her personal information being made available on underground websites.").
[151] *TransUnion*, 594 U.S. at 425. In contrast to the Second Circuit's decision in *Bohnak*, 79 F.4th at 285–86, the court finds it important that the PII was "published" on the dark web, as opposed to simply sitting with a single hacker or hacker group. Without more, where private information "sits in a [cybercriminal's] database" and is not further disclosed on the dark web or otherwise used to commit identity theft or fraud, the plaintiff has suffered no concrete harm. *See TransUnion*, 594 U.S. at 434. Otherwise, every victim of every data breach would arguably have standing to sue even if they suffered no injury from misuse or if the data is returned after a ransom payment. Accordingly, the court concludes that the disclosure of PII is sufficiently comparable to disclosure of private information when the hacker specifically does something with the plaintiff's data, such as publishing it on the dark web or using or selling it to commit identity theft or fraud.

information arrived on the dark web from other sources."[152] In support, Prog primarily relies on *Blood v. Labette County Medical Center*[153] and *C.C. v. Med-Data, Inc.*[154] In *Blood*, the plaintiffs' PII was compromised following a data breach, including their names plus one or more of the following: "Social Security number, medical treatment and diagnosis information, treatment costs, dates of service, prescription information, Medicare or Medicaid number, and/or health insurance information."[155] The plaintiffs alleged that as a result of the data breach, they had unauthorized charges made to their bank account.[156] The court found this allegation to be speculative because plaintiffs "do not plead any facts suggesting how the mere possession of their Social Security numbers and names would enable someone to make unauthorized charges on an existing account (instead of, for example, opening a new account)."[157]

Blood is not comparable to the instant case, as Mr. Maddox, Ms. Williams, and Mr. Hawes do not allege an injury regarding PII not involved in the Data Breach; they simply allege that following the Data Breach, their stolen PII ended up on the dark web. Taking Plaintiffs' allegations as true and affording reasonable inferences, these allegations are sufficient at the motion to dismiss stage given the temporal proximity, that there was no difference in the alleged PII disclosed (unlike in *Blood*), and that the cybercriminals shared a sample of the PII on the dark web.

In *C.C.*, plaintiff's PII, including Social Security number, was "uploaded to a public facing website" following a data breach.[158] Notably, the plaintiff did not allege any misuse of the

[152] Reply in Support of Mot. to Dismiss ("Reply") 3, ECF No. 67, filed August 30, 2024.
[153] No. 5:22-cv-04036-HLT-KGG, 2022 WL 11745549 (D. Kan. Oct. 20, 2022).
[154] No. 21-cv-2301-DDC-GEB, 2022 WL 970862 (D. Kan. Mar. 31, 2022).
[155] *Blood*, 2022 WL 11745549, at *1.
[156] *Id.*
[157] *Id.* at *5.
[158] *C.C.*, 2022 WL 970862, at *1.

data or that it was uploaded to the dark web.[159] As a result, the court held that the plaintiff did not have standing because a "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft."[160] Unlike in *C.C.*, Mr. Maddox, Ms. Williams, and Mr. Hawes allege that their PII was uploaded to the dark web, where "criminals and other malicious actors . . . [go] to carry out technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft."[161]

The First Circuit's traceability analysis in *Webb* is instructive. In *Webb*, the district court held that the plaintiff did not plausibly allege a connection between the data breach and the filing of the false tax return.[162] Reversing this decision, the First Circuit, applying all reasonable inferences in the plaintiff's favor, first pointed to the "obvious temporal connection between the filing of the false tax return and the timing of the data breach."[163] Next, the court reasoned that the allegation was made in the context of allegations relating to harms the plaintiff suffered because of the data breach.[164] The court also credited the allegations that the plaintiff is "very careful about sharing her PII."[165] Accordingly, the court concluded that "[t]he obvious inference to be drawn from these allegations is that the criminal or criminals who filed the false tax return obtained Webb's PII from the . . . data breach, not from some other source."[166]

In this case, the allegations that the PII of Mr. Maddox, Ms. Williams, and Mr. Hawes were placed on the dark web as a result of the Data Breach satisfy traceability. Applying all reasonable inferences in their favor, they allege that their stolen PII from the Data Breach was

---

[159] *See id.* at *7.
[160] *Id.*
[161] *McMorris*, 995 F.3d at 302 n.4 (citing Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1090 (2017)).
[162] *Webb*, 72 F.4th at 373.
[163] *Id.* at 374.
[164] *Id.*
[165] *Id.*
[166] *Id.*

later uploaded on the dark web. These allegations were made in the context of allegations relating to harms the plaintiff suffered because of the data breach. Further, Mr. Maddox and Mr. Hawes allege that they are "very careful about sharing [their] PII."[167] And finally, Plaintiffs allege that the hackers leaked a sample of the stolen PII on the dark web. These allegations, taken together, are sufficient at this stage for the court to conclude that Mr. Maddox, Ms. Williams, and Mr. Hawes have sufficiently pled Article III standing.

2. Standing of Remaining Plaintiffs

Next, the court considers whether the remaining eight Plaintiffs have standing. Among the Alleged-Misuse Plaintiffs, Mr. Boyd alleges that in late September 2023, after the Data Breach, there were "unauthorized charges on his debit card" that he disputed with the bank but "[have] not been reimbursed," causing his account to be overdrawn and resulting in missed payments.[168] Additionally, in October 2023, he noticed approximately fifteen hard inquiries on his credit report, all of which were inaccurate.[169] Second, Ms. Robinson "suffered actual injury in the form of the fraudulent misuse of her compromised PII leading to her bank accounts being frozen without her authorization, with all money in those accounts drained without explanation. Plaintiff Robinson no longer has access to these accounts, nor the funds that were in them."[170] Third, Ms. Ryan "experienced at least two hard inquiries on her credit, received receipts sent to her email relating to items she never purchased, and was forced to spend time getting a new credit card after noticing a series of unauthorized charges on her prior credit card."[171] And fourth, Mr. Alexander alleges that between September 14, 2023 and February 21, 2024, he "has

[167] Compl. ¶¶ 107, 202.
[168] *Id.* ¶ 96.
[169] *Id.* ¶ 97.
[170] *Id.* ¶ 163.
[171] *Id.* ¶ 178.

received multiple notifications indicating that an unauthorized user has attempted to obtain loans" by trying to open accounts with various banks using his PII.[172] He further asserts that the Data Breach and multiple hard inquiries have negatively affected his credit.[173] Additionally, the remaining four Non-Misuse Plaintiffs (who do not allege their information was published on the dark web)— Mr. Dreger, Ms. Davis, Mr. Guzman, and Mr. Whitmore—allege they have suffered an injury in fact based on the potential future disclosure of their PII on the dark web, as well as their increased risk of suffering identity theft or fraud.

The court concludes in line with several other district and circuit courts that the remaining named Plaintiffs have plausibly pled standing at this stage because "the actual misuse of a portion of the stolen information increases the risk that other information [in the same dataset] will be misused in the future."[174] Prog argues that Plaintiffs cannot bootstrap standing based on purported injuries from others as a matter of law.[175] Indeed, "[e]very class member must have Article III standing in order to recover individual damages."[176] This is a correct statement of the law, but it is not what is occurring here. Instead, Plaintiffs plausibly pled a higher likelihood that their own PII will be misused because cybercriminals already have misused other PII in the same dataset.

That multiple Plaintiffs in this case have also experienced unexpected hard inquiries on their credit—while not an injury on its own—plausibly makes the imminence of future misuse of their PII more likely. The same is true regarding Ms. Robinson's allegation that her bank account was frozen and her money drained without explanation.[177] Therefore, in light of the plausible

[172] *Id.* ¶¶ 193–97.
[173] *Id.* ¶ 198.
[174] *Webb*, 72 F.4th at 375.
[175] Reply 6–7.
[176] *TransUnion*, 594 U.S. at 431.
[177] Prog argues that Ms. Robinson's allegations are not fairly traceable to the Data Breach because she does not allege that the numbers for these bank accounts or any security information necessary to access them were provided

allegations of actual misuse by some Plaintiffs, and making reasonable inferences in favor of Plaintiffs, the remaining named Plaintiffs' injury is plausibly imminent and substantial for pleading purposes. Accordingly, unlike in *Clapper*, Plaintiffs' allegations based on time and money spent mitigating the risk of identity theft, fraud, and unauthorized use of their PII[178] sufficiently alleges a concrete injury. All named Plaintiffs therefore have plausibly pled Article III standing for damages.

3. Standing for Injunctive Relief

Under *TransUnion*, "standing is not dispensed in gross; rather, plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)."[179] For injunctive relief as it relates to future harm, a plaintiff "may pursue forward-looking, injunctive relief to prevent harm from occurring at least so long as the risk of harm is sufficiently imminent and substantial."[180] In other words, the harm must be "certainly impending" or at minimum, there must be a "substantial risk" that the harm will occur.[181] Here, the complained of harm supporting an injunction is that Prog will experience another data breach and further compromise Plaintiffs' PII.[182]

---

to Prog. Mot. 20. Although not necessary for the court to decide given that it finds that all remaining Plaintiffs have an imminent and substantial risk of future harm, Plaintiffs allege that their bank routing numbers and checking account numbers were among the PII compromised in the Data Breach. Compl. ¶ 42. With this information, hackers can potentially make fraudulent ACH transfers and payments from the account. *See* Sheryl Nance-Nash, *If Someone Has Your Bank Account Number Can They Take Money Out?*, SoFi (Feb. 27, 2024), https://www.sofi.com/learn/content/what-can-someone-do-with-your-bank-account-and-routing-number/ [https://perma.cc/E73M-3FLM]; Tim Maxwell, *What Can Someone Do With Your Bank Account and Routing Numbers?*, Experian (Jan. 21, 2024), https://www.experian.com/blogs/ask-experian/what-can-someone-do-with-your-bank-account-and-routing-numbers/ [https://perma.cc/DW8K-TK9M]; *see also Instructure, Inc. v. Canvas Techs., Inc.*, No. 2:21-cv-00454-DAK-CMR, 2022 WL 43829, at *18 (D. Utah Jan. 5, 2022) ("It is common practice for courts to take judicial notice of factual information found on the internet.") (citing *O'Tooele v. Northrop Grumman Corp.*, 499 F.3d 1218, 1225 (10th Cir. 2007)). Further, it is a reasonable inference at this stage that the bank account that was allegedly accessed following the Data Breach was the same account provided to Prog.

[178] *See* Compl. ¶ 19.

[179] *See TransUnion*, 594 U.S. at 431.

[180] *Id.* at 435.

[181] *Clapper*, 568 U.S. at 409, 414 n.5.

[182] *See* Compl. ¶¶ 268, 271–74. The court, of course, cannot enjoin the cybercriminal from engaging in further misuse of Plaintiffs' PII.

The court finds that Plaintiffs have failed to plausibly allege that there is a substantial risk of another breach of Prog's systems or that a breach is certainly impending. Plaintiffs allege that, prior to the Data Breach, "Defendant stored the PII of Plaintiffs and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network."[183] They argue that they have plausibly alleged a sufficiently imminent risk of further harm arising from another data breach of Prog's systems because Prog "does not claim to have removed Plaintiffs' PII from the Internet-accessible environment and does not claim to have encrypted Plaintiffs' PII that remains in an Internet-accessible environment."[184] Additionally, the consolidated complaint states that there is an "actual controversy" regarding "whether Defendant is currently maintaining [adequate] data security measures."[185] Plaintiffs allege that Prog's data security measures remain inadequate and Prog publicly denies these allegations.[186]

"Naturally, an injunction requiring [Prog] to improve its cybersecurity systems cannot protect the plaintiffs from future misuse of their PII by the individuals they allege now possess it. Any such relief would safeguard only against a future breach."[187] And the fact allegations in the consolidated complaint do not show that the risk of another data breach is higher than it is at any other entity that holds PII. "If that risk were deemed sufficiently imminent to justify injunctive relief, virtually every company and government agency might be exposed to requests for injunctive relief like the one the plaintiffs seek here."[188] The court cannot conclude, based on the

[183] *Id.* ¶ 6.
[184] Opp'n 16.
[185] Compl. ¶ 268.
[186] *Id.*
[187] *Webb*, 72 F.4th at 378.
[188] *Id*.

allegations of the consolidated complaint, that another data breach of Prog is likely, let alone impending.[189] Accordingly, Plaintiffs have not demonstrated standing to seek injunctive relief.

II. FAILURE TO STATE A CLAIM

The court turns to Prog's contention that Plaintiffs fail to state a claim under Rule 12(b)(6). Plaintiffs assert claims of negligence (Count I), breach of implied contract (Count II), declaratory judgment for injunctive relief (Count III),[190] and violation of the California Consumer Privacy Act ("CCPA") (Count IV).

A. Whether the Court Can, and Should, Consider Prog's Exhibits

In its briefing, Prog cites to several documents not explicitly referenced or attached as an exhibit to the consolidated complaint. Accordingly, the court must first decide whether it can consider these documents.

When evaluating a 12(b)(6) motion to dismiss, the court may consider "not only the complaint itself, but also attached exhibits and documents incorporated into the complaint by reference."[191] When a party presents other categories of documents in a brief, "as a general rule 'the court must either exclude the material or treat the motion as one for summary judgment.'"[192] However, "if a plaintiff does not incorporate by reference or attach a document to its complaint, but the document is referred to in the complaint and is central to the plaintiff's claim, a defendant may submit an indisputably authentic copy to the court to be considered on a motion to dismiss."[193] "When a complaint refers to a document and the document is central to the plaintiff's

[189] *See generally Holmes v. Elephant Ins. Co.*, No. 3:22-cv-00487, 2023 WL 4183380, at *6 (E.D. Va. June 26, 2023) (finding no standing for declaratory and injunctive relief for increased data security measures based only on "conclusory statements" of another possible data breach).
[190] The court has already determined that Plaintiffs do not have standing to seek injunctive relief. *See supra* Section I.D.3.
[191] *Smith v. United States*, 561 F.3d 1090, 98 (10th Cir. 2009) (citations omitted).
[192] *Brokers' Choice of Am., Inc. v. NBC Universal, Inc.*, 861 F.3d 1081, 1103 (10th Cir. 2017) (quoting *Alexander v. Oklahoma*, 382 F.3d 1206, 1214 (10th Cir. 2004)).
[193] *GFF Corp. v. Associated Wholesale Grocers, Inc.*, 130 F.3d 1381, 1385 (10th Cir. 1997).

claim, the plaintiff is obviously on notice of the document's contents, and this rationale for conversion to summary judgment dissipates."[194] The court "has broad discretion in determining whether to accept materials beyond the pleadings."[195]

In the consolidated complaint, Plaintiffs specifically reference and quote at length from Prog's Privacy Policy, dated November 13, 2022, and also attach it as an exhibit.[196] Neither party disputes that the court can properly consider this document.[197] However, in Prog's motion to dismiss, Prog attaches a declaration of Mathew Stout, which attaches certain Application Agreements, including Prog's Application Disclosure Terms, Terms of Use, Arbitration Provision, and various privacy policies dating from October 2015 to the present.[198] Additionally, in its Reply, Prog attaches a second declaration of Mathew Stout, which purports to attach three lease agreements between Prog and Plaintiff Dawn Davis.[199]

Beginning with the documents attached to Prog's Reply, it is well settled that ordinarily, a court will disregard evidence raised for the first time in a reply brief.[200] Prog provides no argument in its brief as to why the court should consider these documents, except for a footnote stating that "Ms. Davis explicitly references her 'active lease[s]' with Prog in the Complaint (Compl. ¶ 116)."[201] Paragraph 116 of the consolidated complaint states in full that "Plaintiff Davis has been a customer of Progressive for approximately four years and currently holds an

---

[194] *Id.*
[195] *Brokers' Choice of Am., Inc.*, 861 F.3d at 1103.
[196] *See* Compl. ¶¶ 3, 257; Privacy Policy, ECF No. 39-1.
[197] *See* Opp'n 18; Reply 9.
[198] First Decl. of Mathew Stout, ECF No. 56-1, filed June 24, 2024.
[199] Second Decl. of Mathew Stout, ECF No. 67-1, filed on August 30, 2024.
[200] *See Sargent v. Utah State Off. of Rehab.*, No. 1:18-CV-44 BCW, 2018 WL 4442237, at *2 (D. Utah Sept. 17, 2018) ("The court typically does not consider issues and arguments raised for the first time in a reply brief, because an opposing party does not have an opportunity to respond to them."); DUCivR 56-1(d) (stating that on summary judgment, "a reply may not contain additional evidence" unless offered to rebut a claim that a material fact is in dispute").
[201] Reply 19 n.13.

active lease." The declaration and lease agreements attached thereto were available to Prog when it filed its motion to dismiss, and consideration of this new evidence "leav[es] the opposing party no opportunity to challenge its validity or relevance."[202] Further, one passing reference to being a current Progressive customer (which necessarily requires an active lease) for the purpose of demonstrating why Prog possessed her PII at the time of the Data Breach is insufficient to supplant the general rule that "[g]enerally, the sufficiency of a complaint must rest on its contents alone."[203] Therefore, the court does not consider these documents.

The court next turns to the documents attached to Prog's motion. First, Prog cites to various privacy policies, particularly the most recent privacy policy dated November 6, 2023.[204] Even if the court could consider this document, it seemingly has no relevance in the instant case given that the Data Breach occurred in September 2023, and Plaintiffs were notified of the breach in October 2023[205] before that version of the privacy policy came into effect. Second, although Prog mentions the Arbitration Provision, Prog does not reference it in its argument or anywhere in its Reply and admits that it is not "relevant to [its] motion to dismiss."[206] Third, Prog does not respond to Plaintiffs' argument that the court should not consider Mathew Stout's declarations themselves (as opposed to the attached exhibits), nor does Prog otherwise mention

---

[202] *W. Coast Life Ins. Co. v. Hoar*, 558 F.3d 1151, 1157 (10th Cir. 2009) (granting motion to strike evidence raised for first time in reply brief).

[203] *Gee v. Pacheco*, 627 F.3d 1178, 1186 (10th Cir. 2010); *see also Doe v. Sarah Lawrence Coll.*, 453 F.Supp.3d 653, 664 (S.D.N.Y. 2020) ("[a] mere passing reference or even references . . . to a document outside of the complaint does not, on its own, incorporate the document into the complaint itself.") (citing *Williams v. Time Warner Inc.*, 440 Fed. App'x 7, 9 (2d Cir. 2011)); *Polanco v. California*, No. 21-CV-06516-CRB, 2022 WL 625076, at *5 (N.D. Cal. Mar. 3, 2022), *aff'd sub nom. Polanco v. Diaz*, 76 F.4th 918 (9th Cir. 2023) (citing *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 999 (9th Cir. 2018)); *Fudge v. Penthouse Int'l, Ltd.*, 840 F.2d 1012, 1015 (1st Cir. 1988) ("Clearly, not every document referred to in a complaint may be considered incorporated by reference and thus introduced by the moving party in support of a motion to dismiss.").

[204] *E.g.*, Mot. 34.

[205] *See* Compl. ¶¶ 7, 9, 13.

[206] *See* Mot. 25–27 (listing only Application Disclosure Terms, Terms of Use, and Privacy Policy in section titled "Relevant Application Agreements"); Reply 9 n.7 (listing only the Application Disclosure Terms, Terms of Use, and Privacy Policy as relevant to its motion to dismiss).

the declarations in its Reply.[207] Therefore, the court treats the issue as conceded and does not consider the declaration.[208]

Accordingly, the only remaining documents for the court to examine—and the focus of the parties' arguments—are the Application Disclosure Terms and Terms of Use that Plaintiffs allegedly agreed to when applying to use Prog's services. Prog advances two arguments as to why the court can consider these documents. First, Prog argues that the consolidated complaint incorporates these documents by reference because Plaintiffs expressly refer to their leases, and the Privacy Policy "expressly incorporates by reference" the Application Disclosure Terms and Terms of Use that govern Prog's services.[209] The paragraphs of the consolidated complaint that Prog refers to state (i) certain terms from the Privacy Policy, (ii) that Prog provides "lease-to-own purchase options," (iii) that Plaintiffs are current or former customers of Prog (which necessarily entails that they held a lease at some point in time), and (iv) that Plaintiff Davis "currently holds an active lease."[210]

As stated above regarding the documents attached to Prog's Reply, these paragraphs referring to Prog's services and Plaintiffs being current or former Prog customers do not detail the actual lease agreements but instead demonstrate why Prog possessed Plaintiffs' PII at the time of the Data Breach. Numerous courts have held, "[a] mere passing reference or even

---

[207] *See generally* Reply 8–11.

[208] *See Bick v. Utah State Univ.*, No. 1:19-cv-00084-DBB, 2021 WL 2379600, at *3 (D. Utah June 10, 2021) ("Because Plaintiff failed to address these arguments, he has conceded this issue."); *see also Nester v. Bank One Corp.*, 224 F.Supp.2d 1344, 1346 (D. Utah 2002) ("It is unquestionably inappropriate to consider plaintiff's affidavit in connection with the 12(b)(6) motion to dismiss since the sufficiency of the complaint is the only issue before the court.").

[209] Mot. 3 n.2; Reply 9–11.

[210] Mot. 3 n.2 (citing Compl. ¶¶ 2–3, 116, 129, 258); Reply 9 (citing Compl. ¶¶ 2, 83, 94, 104, 116, 129, 139, 148, 160, 174, 186.

references . . . to a document outside of the complaint does not, on its own, incorporate the document into the complaint itself."[211] Likewise, the Privacy Policy only mentions the Application Disclosure Terms and Terms of Use once in a single sentence.[212]

Second, Prog argues that the court can consider the Application Disclosure and Terms of Use because Plaintiffs refer to their leases and the Privacy Policy in the consolidated complaint, and they are central to Plaintiffs' claims and authentic.[213] Otherwise, according to Prog, "a plaintiff with a deficient claim could survive a motion to dismiss simply by not attaching a dispositive document" to the consolidated complaint.[214] Notably, Plaintiffs do not dispute the authenticity of these documents in their briefing.

The consolidated complaint does not specifically mention the Application Disclosure Terms or Terms of Use, but it does rely heavily on the Privacy Policy, which Plaintiffs assert is "probative in pleading various causes of action."[215] The Privacy Policy states that the user "should review the Terms of Use, which governs your use of the Progressive Platforms [and] the Application Disclosure, which governs your submission of a rent-to-own application to Progressive."[216]

A review of these Application Agreements demonstrates that they should be considered together. The Application Disclosure Terms are "an agreement between the user and Prog . . . [and] apply to [Prog's] websites, kiosks, software, applications, and other online services that post or include a link to these Terms of Use."[217] The Application Disclosure Terms specifically state that they "include" the Privacy Policy and Terms of Use (among other documents) and

[211] *Doe*, 453 F.Supp.3d at 664; *Polanco*, 2022 WL 625076, at *5; *Fudge*, 840 F.2d at 1015.
[212] Privacy Policy 1.
[213] Mot. 3 n.2; Reply 9–11.
[214] Reply 9.
[215] Opp'n 19.
[216] Privacy Policy 1.
[217] Application Disclosure Terms 1, dated August 26, 2020, ECF No. 56-1 at 6.

"contain the entire understanding between" Prog and the user "with respect to the Progressive Platforms."[218] And by submitting an application with Prog, "the user agrees to be bound by" the Application Disclosure Terms (which also encompass the Privacy Policy and Terms of Use).[219] The Terms of Use similarly state that "[b]y using the Progressive Platforms, the user agrees that he/she . . . will be bound by these Terms."[220] The Terms of Use also refer to the Privacy Policy.[221] Given how intertwined these documents are and that the user must agree to their terms to use the Progressive Platforms, the court does not see how it can review one component of the Application Disclosure Terms (the Privacy Policy) and disregard the remainder of the Application Disclosure Terms and Terms of Use. Therefore, in exercising its "broad discretion,"[222] the court finds that the Application Disclosure Terms and the Terms of Use are central to Plaintiffs' claims through their reliance on the Privacy Policy and will be considered in evaluating Plaintiffs' claims.

B. Breach of Implied Contract

In Count II, Plaintiffs allege Prog required Plaintiffs to provide their PII as a condition of obtaining loans or other products and services from Prog.[223] In providing their PII, Plaintiffs allege that they entered into an implied contract with Prog to safeguard and protect their PII, to keep the PII secure and confidential, and to timely and accurately notify Plaintiffs if their PII had been compromised and stolen.[224] And Prog allegedly breached these contracts "by failing to maintain administrative, technical, and physical safeguards intended to protect against the loss,

[218] *Id.*
[219] *Id.*
[220] Terms of Use 1, dated June 21, 2023, ECF No. 56-1 at 12.
[221] *Id.* ¶ 5.
[222] *See Brokers' Choice of Am., Inc.*, 861 F.3d at 1103.
[223] Compl. ¶¶ 259–60.
[224] Compl. ¶ 261.

misuse, unauthorized access, and disclosure of their PII, failing to take such precautions seriously, and otherwise failing to safeguard and protect their PII."[225]

Prog argues that Plaintiffs cannot assert a claim for breach of implied contract (Count II) because they entered into express contracts with Prog that govern the same obligations or subject matter upon which their implied contract claims are based.[226] Of these express contracts cited by Prog, the court considers the Application Disclosure Terms, the Terms of Use, and the Privacy Policy.

1. Relevant Agreements

The Application Disclosure Terms "are an agreement between the user . . . and Prog . . . [and] apply to [Prog's] websites, kiosks, software, applications, and other online services that post or include a link to these Terms of Use[.]"[227] The document states in all caps: "BY SUBMITTING THIS APPLICATION, THE USER AGREES TO BE BOUND BY THE TERMS SET FORTH BELOW. IF THE USER DOES NOT AGREE WITH THESE TERMS, PLEASE DO NOT SUBMIT THIS APPLICATION."[228] The Application Disclosure Terms include the Terms of Use and Privacy Policy and "contain the entire understanding between" the user and Prog.[229]

The Terms of Use applies to "any use" of the "Progressive Platforms."[230] It "is a legally binding agreement," and "[b]y using the Progressive Platforms, the user agrees that he/she has

[225] Compl. ¶ 263.
[226] Mot. 24–29.
[227] Application Disclosure Terms 1.
[228] *Id.*
[229] *Id.*
[230] Terms of Use 1.

read, . . . understands, . . . [and] will be bound by these Terms."[231] "If the user does not agree with the Terms of Use the user should not use the Progressive Platforms."[232]

Regarding the submission and handling of, and liability for, information provided to Prog in the use of its services, the Terms of Use states the following:

- "The user acknowledges that by submitting Communications to Prog Leasing, no confidential, fiduciary, *contractually implied*, or other relationship is created between the user and Prog Leasing other than pursuant to these Terms of Use and any subsequent written agreement entered into with Prog Leasing."[233]

- PROG LEASING MAKES NO REPRESENTATION OR WARRANTIES OF ANY KIND WHATSOEVER FOR . . . *ANY BREACH OF SECURITY ASSOCIATED WITH THE TRANSMISSION OF SENSITIVE INFORMATION THROUGH THE PROGRESSIVE PLATFORMS*[.]"[234]

- "IN NO EVENT WILL PROG LEASING BE LIABLE FOR ANY LOSS OF PROFITS, BUSINESS, *USE OF DATA* OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND WHETHER BASED IN CONTRACT, NEGLIGENCE OR OTHER TORT."[235]

- "PROG LEASING . . . DISCLAIM[S] AND EXCLUDE[S] LIABILITY FOR *ANY LOSSES AND EXPENSES OF WHATEVER NATURE* AND HOWSOEVER ARISING, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, LOSS OF USE, *LOSS OF DATA*, . . . *LOSS OF OR DAMAGE TO PROPERTY* . . . OR OTHER LOSSES OF ANY KIND OR CHARACTER, *EVEN IF PROG LEASING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES* OR LOSSES, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THE PROGRESSIVE PLATFORMS[.]"[236]

Finally, the Terms of Use specify, in all capital letters, that they "shall be governed by and construed in accordance with the laws of the State of Utah, without regard to conflicts of law provisions."[237]

---

[231] *Id.*
[232] *Id.*
[233] *Id.* § 9 (emphasis added).
[234] *Id.* § 10 (emphasis added).
[235] *Id.* (emphasis added).
[236] *Id.* (emphasis added).
[237] *Id.* § 15.

Turning to the Privacy Policy, section five is titled, "How Do We Protect Your Information?"[238] It states:

> We maintain administrative, technical, and physical safeguards intended to protect against the loss, misuse, unauthorized access, and disclosure of information, including your social security number. *Although we take such precautions seriously, it is impossible for us to guarantee the safety and security of your Information*. Our policies prohibit the unlawful disclosure of Personal Information. . . . *Please note that we do not ensure or warrant the security of any Information that we collect, and you use the Progressive Platforms and our services and provide us with your information at your own risk*.[239]

2. The Application Agreements Bar Plaintiffs' Implied Contract Claims

Plaintiffs do not contest that implied contracts are barred when express agreements cover the subject matter of the litigation.[240] Instead, they argue that "no provision in the agreements other than the Privacy Policy evince a 'meeting of the minds or mutual assent as to the terms of the contract,' especially where representations of data protection are concerned."[241] In doing so, Plaintiffs concede that the Privacy Policy evinces a meeting of the minds or mutual assent as to the terms of the contract with respect to data protection. The court has already recognized that the Application Disclosure Terms includes the Privacy Policy and Terms of Use, and thus an admission as to the Privacy Policy (a part of the Application Disclosure Terms) applies to the Application Agreements as a whole. Moreover, in using the Progressive Platform and applying for a lease, Plaintiffs "agree[d] to be bound by" the Application Disclosure Terms and Terms of Use.[242] The documents cover the subject of data protection,[243] and disclaim the ability to bring implied contract claims. Even the Privacy Policy itself states that "[a]lthough we take such [data

---

[238] Privacy Policy § 5.
[239] *Id.* (emphasis added).
[240] *See* Opp'n 19–22.
[241] Opp'n 19 (citing *In Re Gallagher Data Breach Litigation*, 631 F.Supp.3d 573, 591 (N.D. Ill. 2022)).
[242] Application Disclosure Terms 1; Terms of Use 1.
[243] *See* Terms of Use §§ 9, 10; *see also* Application Disclosure Terms 1 (stating that the Application Disclosure Terms "contain the entire understanding between the user and [Prog] with respect to the Progressive Platforms and no oral or written representation, statement, or inducement not contained herein shall bind either party").

security] precautions seriously, it is impossible for us to guarantee the safety and security of your Information. . . . Please note that we do not ensure or warrant the security of any Information that we collect, and you use the Progressive Platforms and our services and provide us with your information at your own risk.[244] Accordingly, Plaintiffs' implied contract claims are barred due to the existence of the Application Agreements. Count II is dismissed.

C. Negligence

In Count I, Plaintiffs allege that Prog was negligent in safeguarding, securing, and protecting their PII.[245] Prog moves to dismiss this claim under the economic loss rule.[246] Prog applies the economic loss rule under Utah law with a footnote stating that "Plaintiffs do not allege which state's law(s) govern their negligence claims" and Prog reserves the right to supplement or amend its arguments depending on which states' laws Plaintiffs argue are applicable.[247] Plaintiffs respond that their "claims potentially implicate the laws of [11] states" and that "a determination on choice of law is premature because there is an insufficient factual record from which the Court can make a choice of law determination for specific claims."[248] In its Reply, Prog continues to focus on Utah law, albeit with some citations to cases applying the rule under the law of a few other states.[249]

The court cannot decide whether the economic loss doctrine bars Plaintiffs' negligence claim absent a determination of which state's or states' laws apply. The parties have not made

[244] Privacy Policy § 5.
[245] Compl. ¶¶ 229–256.
[246] Mot. 31–35.
[247] Mot. 31 n.8.
[248] Opp'n 25.
[249] Reply 15–17.

any serious attempt to brief this issue. Accordingly, the court denies Prog's motion to dismiss Count I.[250]

D. California Consumer Privacy Act ("CCPA")

In Count IV, Plaintiffs allege that the Data Breach entitles Plaintiff Davis and the California Subclass members to recover damages under the CCPA.[251] Prog moves to dismiss this claim for failure to provide proper pre-suit notice for statutory damages and because Plaintiff Davis has not alleged any "actual" damages recoverable under the CCPA.[252]

The CCPA provides a right of action for consumers whose "nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures[.]"[253] It allows recovery of statutory damages (between $100 and $750 per consumer per incident) or actual damages, whichever is greater.[254] The consumer must provide a business 30 days' written notice identifying the specific provisions of the CCPA the consumer alleges were violated "prior to initiating any action against a business for statutory damages."[255]

On November 13, 2023, Plaintiff Davis provided written notice to Prog, identifying the specific provisions of the CCPA that she alleges have been or are being violated.[256] However, on this same day, Plaintiff Davis filed a class action complaint in the U.S. District Court for the Central District of California (the "California Complaint") asserting claims against Prog for its

[250] If Prog chooses to move to dismiss this claim again, the parties must provide briefing on the choice of law issues. Of course, the parties may choose to stipulate to which state's law the court should apply or whether there are meaningful differences in the economic loss doctrines of the applicable states.
[251] Compl. ¶¶ 275–83.
[252] Mot. 38–40.
[253] Cal. Civ. Code § 1798.150(a)(1).
[254] *Id.*
[255] *Id.* § 1798.150(b).
[256] Compl. ¶ 283; CCPA Notice Letter, ECF 64-2.

alleged violation of the CCPA.[257] As such, Prog alleges that Plaintiff Davis failed to provide proper pre-suit notice. Plaintiffs respond by pointing out that the CCPA's notice provision only applies "prior to initiating any action against a business *for statutory damages*,"[258] and the California Complaint only sought pecuniary damages.[259] The California Complaint further explained that "[i]f Defendant fails to cure this breach pursuant to §1798.150(b), Plaintiff may seek to amend this Complaint to also seek statutory damages."[260]

Prog argues that Plaintiff Davis's actions reflect a "purported loophole in the statute" that the court should reject.[261] It contends that "[t]he California legislature did not intend such an end-run around the plain text of the CCPA, which was clearly designed to 'allow the defendant an opportunity to cure the [alleged] defect outside of court' and without the threat of a pending lawsuit."[262] Prog primarily relies on *Griffey v. Magellan Health Inc.*,[263] in which the plaintiff provided notice of a CCPA violation three days before filing a lawsuit that did not seek statutory damages.[264] More than 30 days later, the plaintiff filed a second amended complaint that included statutory damages.[265] The U.S. District Court for the District of Arizona dismissed the plaintiff's CCPA claim, finding that the plaintiff "cannot supplement the time between the notice and the initiation of the lawsuit by amending his complaint," which would render the pre-suit

[257] Cal. Compl., ECF No. 56-2.
[258] Cal. Civ. Code § 1798.150(b) (emphasis added).
[259] Opp'n 35; Cal. Compl. ¶ 60 ("Plaintiff, on behalf of herself and all other members of the Class, seeks actual damages.").
[260] Opp'n 35; Cal. Compl. ¶ 61.
[261] Reply 17–18.
[262] *Id.* at 17 (citing *Griffey v. Magellan Health Inc.*, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022)).
[263] No. 20-cv-01282-PHX-MTL, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022).
[264] *Id.* at *6.
[265] *Id.*

notice requirement "pointless."[266] The court reasoned that the purpose of the CCPA's pre-suit notice is "to allow the defendant an opportunity to cure the defect outside of court."[267]

To be sure, this reasoning does have some appeal. However, it appears to conflict with the plain text of the statute. The CCPA specifically states that "[n]o notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title."[268] It specifies that pre-suit notice is only required "prior to initiating any action against a business *for statutory damages*."[269] Given that Plaintiff Davis's California Complaint did not seek statutory damages, and she only sought statutory damages after the 30 day notice period, it appears that Plaintiff Davis complied with the CCPA. A California state court recently came to the same conclusion when faced with a nearly identical argument.[270]

Prog provides an additional argument that Plaintiff Davis's demand letter was insufficient because it "merely quoted the statute without any factual detail about Prog's purported failure to implement and maintain reasonable security practices."[271] It is true that the CCPA Notice Letter provides minimal factual details. It states that "[a]s a result of the Data Breach, nonredacted and nonencrypted PI[I] of customers that was stored on [Prog's] servers was compromised, accessed, and subject to exfiltration, theft or disclosure."[272] After citing relevant provisions of the CCPA, the Letter continues, "[y]ou have failed to protect customers' PI from the Data Breach and have

[266] *Id.*
[267] *Id.* (citing *T & M Solar & Air Conditioning, Inc. v. Lennox Int'l Inc.*, 83 F. Supp. 3d 855, 875 (N.D. Cal. 2015)).
[268] Cal. Civ. Code § 1798.150(b).
[269] *Id.* (emphasis added).
[270] *See Bohannon v. Lyon Real Estate*, Hearing Minutes at 14–15, ECF No. 64-1.
[271] Reply 19.
[272] CCPA Notice Letter 1.

"violat[ed] [your] duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[273]

However, the plain text of the CCPA only requires "written notice identifying the specific provisions of this title the consumer alleges have been or are being violated."[274] Plaintiff Davis has done so. Identification of specific security deficiencies in the demand letter is not required by the statute, and in fact, the CCPA was amended on January 1, 2023 to clarify that even "[t]he implementation and maintenance of reasonable security procedures and practices . . . following a breach does not constitute a cure with respect to that breach.[275] Prog's cited cases in support of this argument were each decided prior to this amendment and generally held that the complaint must allege facts to support the notion that the defendant's security was deficient.[276] Plaintiffs' consolidated complaint does so.[277] Therefore, the court finds that Plaintiff Davis complied with the CCPA's pre-suit notice requirement.

Prog also argues that Plaintiff Davis has not alleged "actual pecuniary damages" under the CCPA, which Prog contends are limited to out-of-pocket expenses.[278] Plaintiffs respond that Plaintiff Davis's allegation that she "lost time" attempting to mitigate the actual consequences of the Data Breach are sufficient.[279] Specifically, Plaintiff Davis alleges that she "made reasonable efforts to mitigate the impact of the Data Breach, which required her to expend significant

---

[273] *Id.* at 2.
[274] Cal. Civ. Code § 1798.150(b).
[275] *Id.*; *see also In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022) (rejecting argument that plaintiff needed to allege a specific action defendants took or failed to take that breached a duty under the CCPA to maintain "reasonable" security measures at the motion to dismiss stage) (citing *Mehta v. Robinhood Fin. LLC*, No. 21-cv-01013-SVK, 2021 WL 6882377, at *8 (N.D. Cal. May 6, 2021)).
[276] *See Magellan Health Inc.*, 562 F. Supp. 3d at 57; *In re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *6 (S.D.N.Y. Feb. 24, 2022); *Maag v. U.S. Bank, Nat'l Ass'n*, 2021 WL 5605278, at *2 (S.D. Cal. Apr. 8, 2021); *In re Canon U.S.A. Data Breach Litig.*, No. 20-cv-6239-AMD-SJB, 2022 WL 22248656, at *13 (E.D.N.Y. Mar. 15, 2022).
[277] *See, e.g.*, Compl. ¶¶ 54–57, 62–67.
[278] Mot. 40–41.
[279] Opp'n 37.

time—valuable time Plaintiff Davis otherwise would have spent on other activities, including but not limited to work and/or recreation."[280] In support of this argument, Plaintiffs cite to *In re Arthur J. Gallagher Data Breach Litig.*,[281] in which the U.S. District Court for the Northern District of Illinois considered whether allegations of lost time responding to a Data Breach constituted an economic injury under several California consumer protection statutes, including the CCPA.[282] The court concluded that the California plaintiffs adequately alleged damages because California "state courts have said that significant time and paperwork costs incurred to rectify violations also can qualify as economic losses."[283]

In contrast, Prog cites to *Griffey v. Magellan Health Inc.*,[284] in which the U.S. District Court for the District of Arizona rejected the plaintiff's argument that lost money or property constitutes actual pecuniary damages under the CCPA because the plaintiff "alleges no out-of-pocket expenses."[285] Additionally, the court in *Holly v. Alta Newport Hospital, Inc.*,[286] found allegations of lost "time and expenses mitigating and remediating the increased risk of identity theft and identity fraud" following a data breach were too "conclusory and vague" to establish actual damages for breach of contract and negligence claims.[287] And finally, Prog cites to *Pruchnicki v. Envision Healthcare Corp.*,[288] which—after examining multiple California district court cases regarding allegations of lost time—held that "tangible, out-of-pocket expenses are required in order for lost time spent monitoring credit to be cognizable as damages" on the plaintiff's negligence, breach of implied contract, negligent misrepresentation, and Nevada

[280] Compl. ¶¶ 121–22, 125.
[281] 631 F. Supp. 3d 573 (N.D. Ill. 2022).
[282] *Id.* at 588.
[283] *Id.* (quoting *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 829 (7th Cir. 2018)).
[284] 562 F.Supp.3d 34 (D. Ariz. 2021).
[285] *Id.* at 57.
[286] 612 F. Supp. 3d 1017 (C.D. Cal. 2020).
[287] *Id.* at 1026.
[288] 439 F. Supp. 3d 1226 (D. Nev. 2020), *aff'd*, 845 F. App'x 613 (9th Cir. 2021).

consumer fraud statute claims.[289] The Ninth Circuit affirmed this dismissal on de novo review—albeit in an unpublished decision.[290]

The court concludes that summary allegations of lost time unaccompanied by out-of-pocket expenses are insufficient to establish actual pecuniary damages under the CCPA. The CCPA instead affords these plaintiffs the ability to recover statutory damages. Accordingly, Plaintiff Davis may only recover statutory damages under the CCPA.

E. Declaratory Judgment

In Count III, Plaintiffs seek a Declaratory Judgment regarding whether Prog is currently maintaining data security measures adequate to protect Plaintiffs from further data breaches.[291] Specifically, Plaintiffs ask the court to declare that Prog "owes a legal duty to secure" Plaintiffs' PII, that Prog is in breach of this duty by "failing to employ reasonable measures to secure" their information, and that failure has caused harm to Plaintiffs.[292] Prog argues that Plaintiffs' request for declaratory relief is merely duplicative of its other claims and should be dismissed.[293]

Federal courts have broad discretion in granting or denying declaratory relief.[294] Several courts have held that such duplicative claims for declaratory relief warrants dismissal.[295] Plaintiffs respond that their declaratory relief claim seeks to prevent future injuries, while their other claims seek to remedy Plaintiffs' past and current injuries resulting from the Data

---

[289] *Id.* at 1233.
[290] *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613, 614 (9th Cir. 2021).
[291] Compl. ¶ 268.
[292] Compl. ¶ 270. Plaintiffs also seek "corresponding prospective injunctive relief requiring [Prog] to employ adequate security protocols . . . to protect consumers' PII." Compl. ¶ 271. But the court has already determined that Plaintiffs do not have standing to seek injunctive relief.
[293] Mot. 41–42.
[294] *Wilton v. Seven Falls Co.*, 515 U.S. 277, 289-90 (1995); *Burger v. Healthcare Mgmt. Sols., LLC*, No. 23-cv-1215-RDB, 2024 WL 473735, at *9 (D. Md. Feb. 7, 2024).
[295] *See* Mot. 41–42 (citing *Chevron U.S.A. Inc. v. Apex Oil Co., Inc.*, 113 F. Supp. 3d 807, 824 (D. Md. 2015); *Scott v. Conley*, 2016 WL 4257507, at *8 (D. Utah July 18, 2016); *Warnick v. Briggs*, 2005 WL 1566669, at *9 (D. Utah July 1, 2005) and *Burger*, 2024 WL 473735, at *9).

Breach.[296] They argue that "Plaintiffs are entitled to seek declaratory and injunctive relief requiring Defendant to implement proper data security measures consistent with applicable law and industry standards to protect their data privacy interests."[297] But this remedy to prevent future injuries appears no different than Plaintiffs' claim for injunctive relief for which they have no standing. "The Declaratory Judgment count therefore serves no purpose other than to reiterate the injunctive relief requested in [Plaintiffs'] other counts, as it is based on the same alleged breach of duty and harm stated in the other counts."[298] Accordingly, the court dismisses the remainder of Count III.

ORDER

It is hereby **ORDERED** that Prog's Motion to Dismiss Plaintiffs' Complaint is **GRANTED IN PART** and **DENIED IN PART**. The court **FURTHER ORDERS** that Counts II and III are **DISMISSED without prejudice**.

Signed January 16, 2025.

BY THE COURT

David Barlow
United States District Judge

[296] Opp'n 38.
[297] *Id.*
[298] *Burger*, 2024 WL 473735, at *9.